United States
Mission Control Center
(USMCC)

Functional Description Document

1 October 2005

Version 2.0

Table of Contents

List of Figures

List of Tables

Deleted: Section Break (Next Page)

United States Mission Control Center (USMCC)

Functional Description Document

1 Introduction

1.1 General

The Functional Description Document (FDD) provides a brief summary description of the major hardware components and software processes used by the United States Mission Control Center (USMCC). The main purpose of the USMCC is to process information from emergency beacons that are detected by satellites and processed by Local User Terminals (LUTs), and to relay results to appropriate Search and Rescue (SAR) authorities. The USMCC operates as part of the United States Sarsat Ground System which, in turn, is part of the international Cospas-Sarsat search and rescue satellite system.

The USMCC is operated by the National Oceanic and Atmospheric Administration (NOAA) on behalf of the U.S. Department of Commerce. The equipment described herein is located at the NOAA Satellite Operations Facility (NSOF) in Suitland, Maryland. The system consists of a series of Intel based servers that perform specific function(s) and exchange processed information.

1.2 Overview

The USMCC is based upon detailed requirements that are described in the Functional Requirements Document (FRD). It consists of 12 sub-systems that are identified in the FRD and listed in Table 1.

Figure 1-1 depicts the relationship between the various sub-systems. These 12 sub-systems are distributed over several processing groups that are separated through firewall segmentation to protect the USMCC from unauthorized intrusion and corruption. These processing groups include:

- **MCC processing** – provides the main processing capability for Cospas-Sarsat related data (MCC Operational Segment)
- **Web application processing** – provides internet access and processing for the RGDB and IHDB functions (Web Based Registration and Related Systems)

- **FTP processing** – provides FTP & fax communications services for international points-of-contact (MCCs & SPOCs) and the Air Force Rescue Coordination Center (AFRCC) (FTP Internet Segment)

- **LUT FTP processing** – provides FTP communication services for US LUTs and Coast Guard RCCs (LutFTP Segment)

The majority of these functions are duplicated at the remote offsite USMCC located at SSAI Headquarters in the Aerospace Building in Lanham, Maryland. Figure 1-2 provides the topology for the USMCC processing and communication facility. Sections 2 and 3 of this document provide a brief summary description of each function and hardware item.

The Detailed Design Document (DDD) contains more detailed descriptions and diagrams that depict the relationship between units, control elements, data flow, validation, exception handling and dynamic tasks. The Baseline Source Document (BSD) describes input, output, configuration and source code files together with installation and initialization procedures.

Figure 1-3 provides the topology for the remote offsite USMCC.

No	Sub-system	Functions	Acronym
1	Alert Processing	Validation, Match/Merge, Message Content, Message Destination	ALRT
2	Communication	Receipt, Data Formatting & Distribution	COMM
3	Operator Interface	Provides capability for controller to monitor/operate the USMCC	OPER
4	System Data	Telemetry & Orbit Vector Processing, Spacecraft Commands and Narrative Messages	SDAT
5	System Monitoring	LUT, MCC and Satellite Performance, Large Location Error Reporting	SMON
6	Registration Database	Entry, Confirmation Process, Report Generation for 406 MHz beacon registration data	RGDB
7	Incident History Database	Entry, Report Generation of SAR incident data	IHDB
8	Self-test & Monitoring	LUT, MCC satellite and beacon Availability, Performance, Statistical Reports	SAMS
9	LUT Monitoring Database	LUT monitoring, Availability, Contract Accounting	LMDB
10	Interference Monitoring	Interference Match/Merge, Report Generation	INTF
11	Database Maintenance	Archive, Purge, Backup, Database Performance	DBMN
12	SAR Mapping and Geo-sort	Map displays, Geo-Sort, Region Definitions	SMAP

Table 1: USMCC Subsystems

1.3 Reference Documents

The following documents contain additional information about the USMCC and its functional processes:

- USMCC Baseline Source Document (BSD). *This document contains details about the software modules of the USMCC*
- C/S A.001, Cospas-Sarsat Data Distribution Plan. *This document defines validation, filtering and routing procedures for messages exchanged with other Cospas-Sarsat MCCs and SPOCs.*
- C/S A.002, Cospas-Sarsat Standard Interface Document. *This document defines message formats and communication standards that are used by Cospas-Sarsat MCCs for international data exchange*
- C/S A.003, Cospas-Sarsat System Monitoring and Reporting. This document provides international system monitoring and reporting requirements for MCCs.
- C/S A.005, Cospas-Sarsat Mission Control Center Performance Specification and Design Guidelines. *This document details the international specifications for MCCs.*
- USMCC Detailed Design Document (DDD). *This document contains details on the software and data processes of the USMCC*
- USMCC Data Structures Document. *This document lists the details for every SQL database table and field used by the USMCC...*
- National Cospas-Sarsat Network Interface Specifications (NTS). *This document defines the message format for data exchange between the USMCC and its LUTs.*
- USMCC Functional Requirements Document (FRD). *This document outlines the essential requirements of the USMCC*
- USMCC Operating Instructions (UOI). *This document provides a detailed description of the screen formats and functionality that are used by the USMCC Operator Interface subsystem*
- United States Mission Control Center (USMCC) National Rescue Coordination Center (RCC) and Search and Rescue Point of Contact (SPOC) Alert and Support Messages. *This document describes the format and content for messages that are sent to the national RCCs and SPOCs and international SPOCs.*

Deleted: *filtering and*

Deleted: ..

- Telemetry and Command Procedures (TCP). This document contains guidance on handling spacecraft telemetry data and commanding procedures.

- CEMSCS/IPD[1] Data Interface. *This document describes the data format and the data exchange procedures between CEMSCS/IPD and the USMCC for Telemetry data*.

[1]Central Environmental Meteorological Satellite Computer System / Information Processing Division.

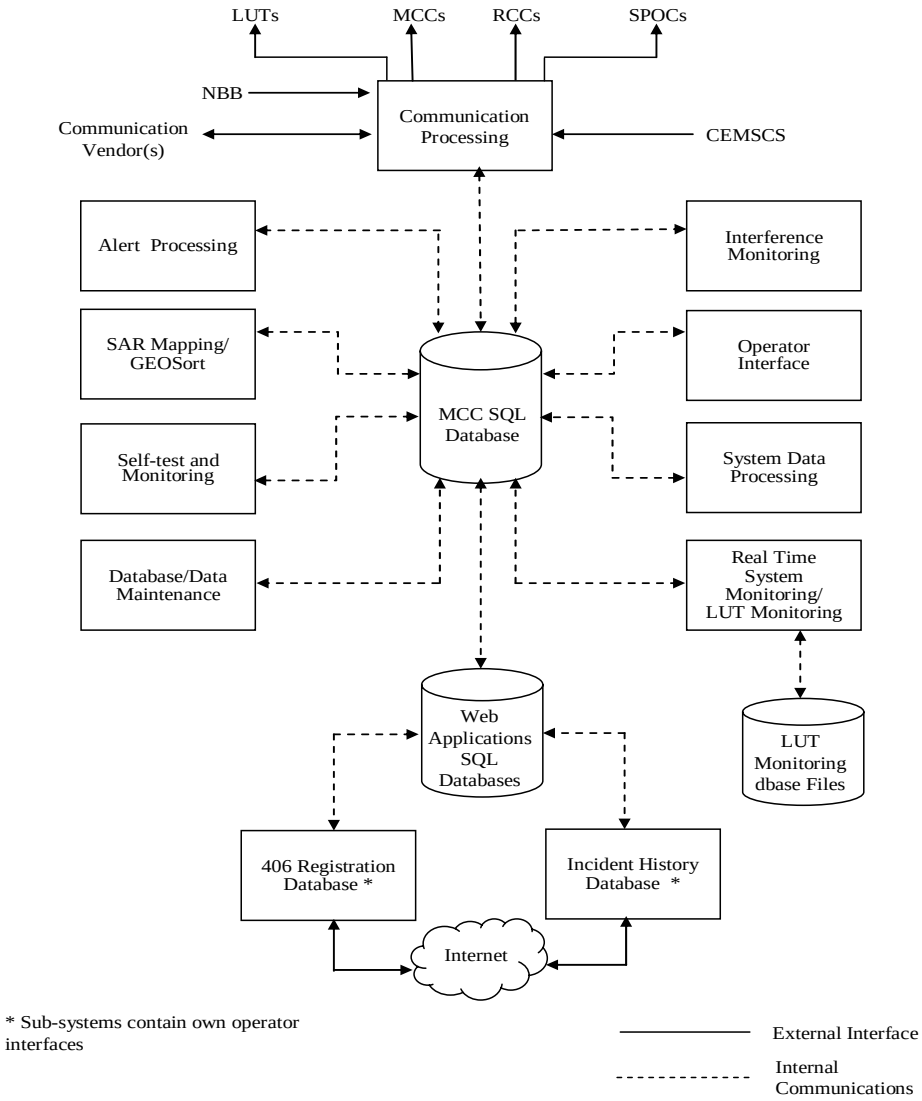

Figure 1-1: USMCC Functional Description

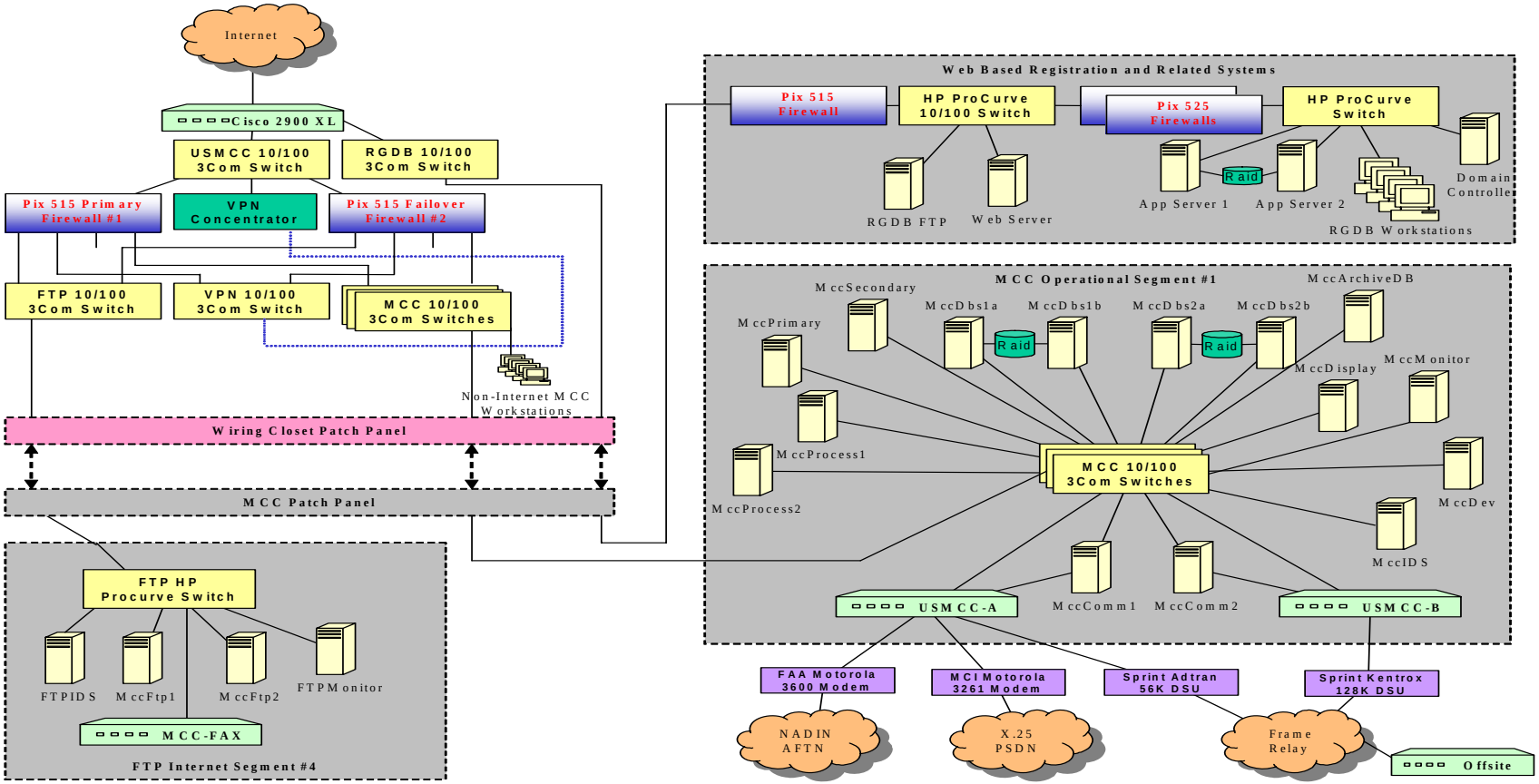

Figure 1-2: USMCC Functional Hardware Description

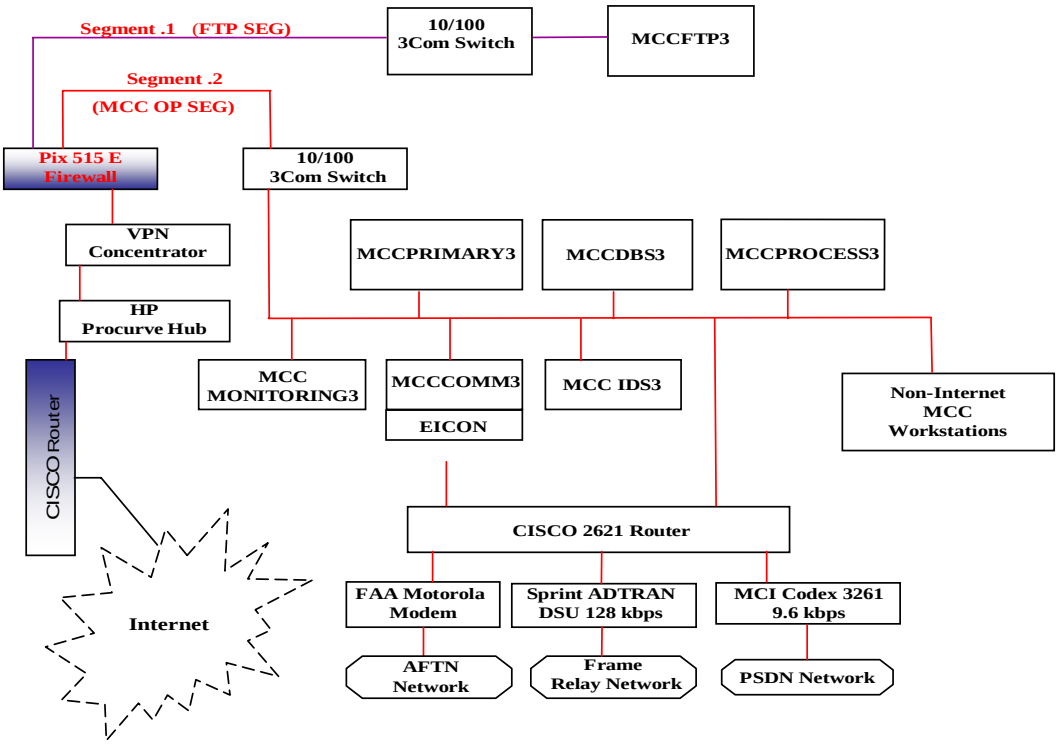

Figure 1-3: USMCC Offsite Processing and Communications Facilities

2 Software Functional Description

2.1 COTS and System Software

2.1.1 Microsoft SQL

In Figure 1-1, the MCC SQL (Structured Query Language) database is shown at the center of the figure, with all the other processes connected to it. The Microsoft SQL server is the focal point for other MCC processes because it:

a) stores data records that are received from, produced by, or passed to the other processors;
b) stores configuration information that is used by other processors such as primary communication circuit and circuit information for a particular communication destination; and
c) performs some data validation when data is stored within a database field.

Deleted: stores

For example, when a message is received from a United States LUT, it is stored in a database table for incoming messages; other database fields are used to indicate the type of message that was received and whether or not it has been processed. Functions that handle incoming messages periodically check the table to determine whether there is any new data to be processed. As additional processing is completed, the results are written to specific output tables. Similar procedures are used throughout the system. Some functions read configuration from SQL tables before executing. Limited data validation is achieved by defining acceptable values or numeric ranges for data that is inserted into various database fields. Values are checked when data is written to the SQL database table.

A comprehensive description of all SQL database tables used by the USMCC is contained in the Data Structures Document. Data formats that are used internally by the USMCC are defined in this document together with acceptable values. The field definitions contained in this document serve as a data definition dictionary. Definition of and modification to SQL tables is subject to configuration management review and approval process.

Because the SQL server plays such a critical role, data is mirrored on another disk drive (Section 3).

2.1.2 Operating Systems

Microsoft Windows provides the operating system software on which the USMCC applications software run. Windows services are used to ensure that applications can always run, even if a user is not logged on. Windows registries provide configuration parameters for Windows services and for application software.

2.1.3 Faxman

Faxman is a COTS used to provide facsimile service for data communication. When the USMCC communications module determines that a communication site is configured to receive messages via fax, the Faxman software is accessed to provide the proper configuration and protocol to allow the message to be transmitted via analog telephone lines connected to the facsimile router in the FTP processing segment.

2.1.4 Web Based COTs and Open Source Components

Name	Type	Description
Macromedia JRun	COTS	Provides the Java Virtual Machine environment that supports the main IBRD application. (includes Macromedia Type IV JDBC Driver for Microsoft SQL Server)
Java SDK	open source	Provides the underlying Java Runtime Environment (JRE) used by JRun4.
Apache HTTP Server	open source	Provides the HTTP Server – version with SSL support (mod_ssl) is required.
Jacob.jar	open source	This Java Archive (JAR) package provides a JAva-COm-Bridge (Jacob) which allows calls to COM Automation components from within Java code. It uses the Java Native Interface (JNI) to make calls into the COM and Win32 libraries (used for calling Beacon Decode DLL).
Jacob.dll	open source	Dynamic Link Library (DLL) associated and used with Jacob.jar to support Win32 library.
Xerces.jar	open source	This is an Parser which reads in eXtensible Markup Language (XML) and extracts tags and elements accordingly
Log4J-1.2.4.jar	open source	Logging package containing an API that provides detailed context for application error or exception logging.
mail.jar	open source	JavaMail packages which provides facilities for reading and sending email and supports multiple protocols and service providers including SMTP, IMAP and POP3
activation.jar	open source	Used in association with the above JavaMail API. The activation.jar contains Java class files as part of the JavaBeans Activation Framework (JAF)
J2EE.jar	open source	Core Library Package for J2EE applications.

2.1.5 Security COTs

2.1.5.1 ITS Real Secure Networks Sensor

2.1.5.2 Audit Wizard

2.1.5.3 Shavlik

2.1.6 Backup COTS

2.1.6.1 Veritas

2.1.6.2 Backup Exec Server

2.1.7 Crystal Reports

Provides reporting capability as part of the Incident History Data Base System. There are two parts to the Crystal Reports COTS, one is the Report Designer and the other is the Report Application Server (RAS). The Report Designer is the GUI for creating and formatting report files which have a .rpt extention. These files are saved on the machine where the Report Application Server is running and the RAS is configured to access these files. The job of the RAS is to generate formatted reports at runtime using data from the database and the report files. The finished report is passed to the JRun Application Server for display to the user. The Java API for communicating with the RAS is implemented through the use of jar (Java Archive) files that are distributed with the Crystal report installation.

2.1.8 Time Service

2.1.9 MapInfo

MapInfo is used to define geographic boundaries for search and rescue regions. It is also used by the Alert Processing subsystem to geographically sort data and determine a corresponding organization responsible for a given search and rescue region. Lastly, it is used as a geographical information service to display active alerts.

2.1.10 Other Software Products

Most USMCC software was developed using Microsoft Visual Studio as the software development environment, with Visual C++ and Visual Basic as programming languages. Various client tools for interfacing with the SQL Server, such as Query Analyzer and Enterprize Manager are used as well for analysis, database maintenance and generation of SQL Stored Procedures.

2.2 Software Subsystems

2.2.1 Alert Processing

The functions carried out in Alert Processing are shown in Figure 2-1. It consists of a series of ten sub-processes, identified by the oval boxes, which are executed in sequence. In addition to the ten sub-processes, the Figure shows the relationship of the sub-processes to the SQL data base and the SMAP function. The Message Type List shown is an internal table.

The sub-processes are described briefly as follows:

2.2.1.1 Data Transfer

The Transfer sub-process: (1) converts data from the Input Message tables of the SQL Database to Input Data Items; (2) groups the Input Data Items into Data Processing Groups (DPGs); (3) assigns a Processing Time to each DPG; and, (4) passes the DPGs to the Validation sub-processes. The Transfer also performs some elementary checks on the data and, if necessary, attaches one or more Control Codes to the DPG.

Deleted: ¶
¶

2.2.1.2 Data Validation

Data Validation consists of checks applied to selected parameters in each Input Data Item (IDI) of a Data Processing Group (DPG). The parameters are specified in the Alert Validation Configuration tables of the SQL Database. The tables list: (1) the ValidationID (CheckCode); (2) the name and units of the parameter to be checked; (3) the limits or discrete values allowed for the parameter; and, (4) the actions to be taken if the test fails. Data Validation is performed separately for data received from US LUTs and for data received from foreign MCCs.

Message Validation procedures are broader than Data Validation procedures in that they cover more than one field at once and may include some pre-processing. Validation is performed for reasonableness, self-consistency, agreement with the C/S A.001 and C/S A.002 agreement with USMCC information, and normal value ranges.

For each validation condition that fails a Control Code is added to the Input Data Item. The Control Codes give special instructions used by the Alert process to guide match, merge and message routing processing.

2.2.1.3 Data Classification

This sub-process breaks down the Input Data Items into Alert Data Items (ADI) for Match/Merge Processing. The ADI Type Code is a four-bit code associated with the ADI. The code bits indicate the information content of the ADI, as shown in the following table. These four-bit codes guide the processing of the ADI through Match/Merge.

Bit	Information in ADI	0 means	1 means:
0	Beacon ID	121.5/243-MHz	406-MHz
1	EventTime	GEO	LEO
2	DopplerLocation	Unlocated	Doppler
3	EncodedLocation	No encoded	Encoded

There are seven possible combinations of the above four beacon types. They are listed below with their type code.
0110 – 123 Leo Doppler.
1000 – 406 Geo No Doppler No Encoded
1100 – 406 Leo No Doppler No Encoded
1001 – 406 Geo No Doppler Encoded
1101 – 406 Leo No Doppler Encoded
1110 – 406 Leo Doppler No Encoded
1111 – 406 Leo Doppler Encoded.

2.2.1.4 Data Filtering

This sub-process checks the Input Data Items against Configuration Parameters and attaches Contro Codes (similar to Validation) for Special Processing, Exceptions Processing, Match/Merge Processing, Site Maintenance, Message Routing, Message Formation, and other Alert sub-processes as required. Special Processing and Exceptions Processing involve a comparison of incoming data against entries in alert configuration tables that identify action to be undertaken. The Data Structures Document and FRD documents contain further details on this subject.

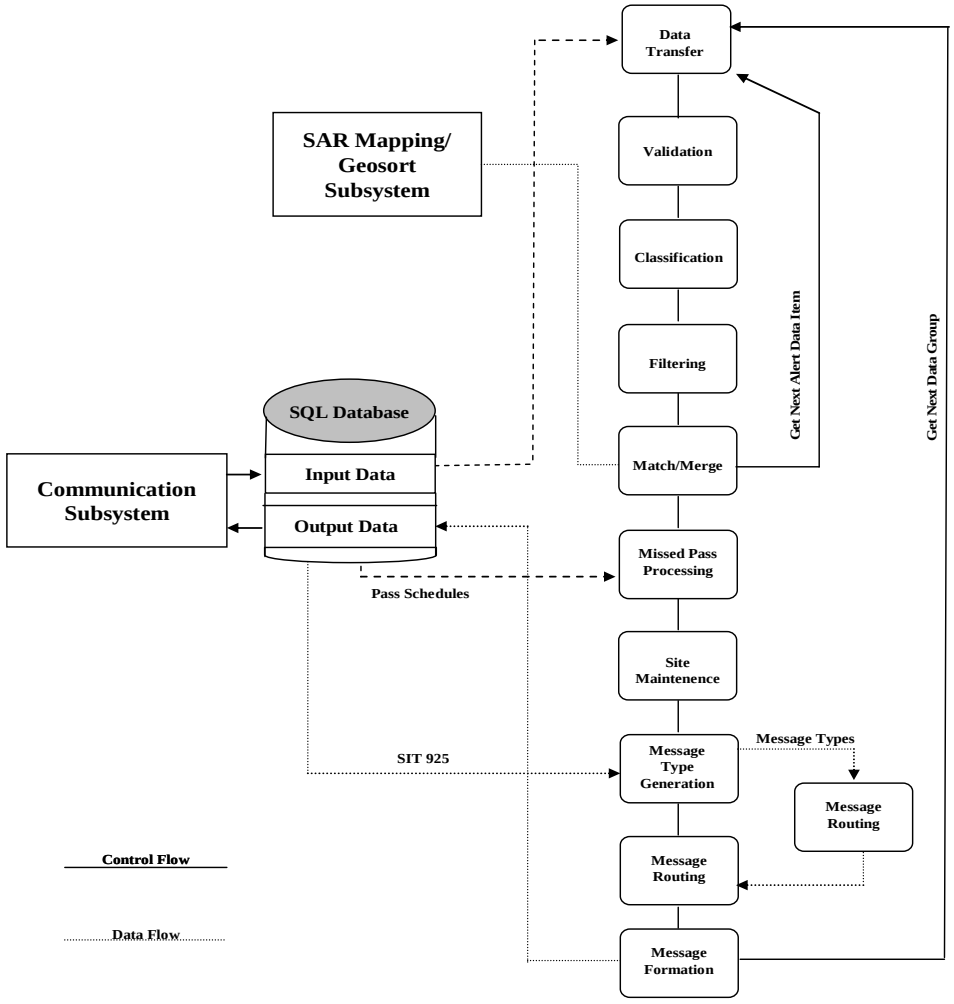

Figure 2-1: Alert Process Overview

2.2.1.5 Match/Merge

This sub-process matches and merges Alert Data Items into the 121.5/243-MHz Alert Sites and the 406-MHz Alert Sites. The Alert Data Items are first checked for any Control Codes that may affect processing, such as whether to process or supress the data or whether there is any special routing for a Data Item. If the data is to be processed, it is checked to determine whether or not the data matches data recorded in an existing site. If no match is found, a new site is created. If a match is found, the data is merged into the site as either new or redundant information. The basic criteria used to determine whether data is new or redundant is described in C/S A.001. The creation of a new site will trigger a first alert message. Updates to a site (new satellite pass data) will cause ambiguity resolution or continued composite message types (see 2.2.1.8) to be produced, depending upon the current status of the alert site. Even if a message is not generated site summary information such as location or frequency may be updated. A more detailed description of messages may be found in C/S A.002 (messages to MCCs) and the USMCC RCC and SPOC Alert Support Messages document.

2.2.1.6 Missed Pass Computation

This sub-process computes the missed pass information for USMCC alert messages. The Missed Pass computation is performed when all ADIs of a US LUT Data Processing Group have been processed. The process is the same for 121.5/243-MHz as for 406-MHz beacons.

2.2.1.7 Site Maintenance

This sub-process includes Site Frequency Determination (updates site frequency), Site Closing Conditions, and extraction of data for the Morning Report and Incident History Database, and other housekeeping functions. When a USMCC controller requests that an alert site be closed, the Alert process generates an Input message that it later processes to close the site.

Deleted: extraction

Deleted: ¶
¶

2.2.1.8 Message Type Generation

The Message Type Generation sub-process modifies some of the Message Types produced by Match/Merge, and adds several other Message Types based on the results of the Match/Merge, Missed Pass and Site Maintenance sub-processes. These include Better A-B, Position Conflicts, Detection Update, Image Position Determination, NOCR, 406 MHz Beacon Registration [Subject Indicator Type (SIT) 925], Missed Pass, and Site Closing Message Types.

At the end of the Message Type Generation sub-process, a Message Type list is passed to Message Routing.

2.2.1.9 Message Routing

Message Routing (1) determines the destination list for the Alert Message Types produced by Message Type Generation and (2) specifies the contents of the Alert Message Routing list.

Message Routing includes the Alert Site Send Checks, the SAR Table Send Checks, SAR Table Trace Procedures, the SAR Table Echo Procedures and the Delay 121 First Alert Procedure.

2.2.1.10 Message Formation

This sub-process forms the USMCC alert message types based on the results of Alert Message Routing and the data in the Alert Site and places them in Output message tables for transmission by Communications. It includes Next Pass Computation for use on the Output Messages. (See section 2.2.3.6 for narrative messages handling).

2.2.2 Communications

The communication function processes incoming and outgoing messages. Two way data communication occurs between the USMCC and the United States Local User Terminals (LUTs), other Cospas-Sarsat Mission Control Centers (MCCs), and with communication vendors. Generally one way communication occurs from the USMCC to United States Rescue Coordination Centers (RCCs), and to foreign SPOCs. Orbit vector information for Cospas-Sarsat satellites is received from the Naval Bulletin Board (NBB), and telemetry data is received from Central Environmental Meteorological Satellite Computer System (CEMSCS) for NOAA satellites. The USMCC employs a variety of secure and non-secure communication protocols to exchange data:

- FTP over Sprint Frame Relay is used to communicate with the US Coast Guard, RCCs and the US LUTs

- FTP over VPN is used to communicate with MCCs and the AFRCC and as a backup for the USCG RCCs

- X.25
  - Over Sprint Frame Relay is used as backup communications with the AFRCC
  - Over the Federal Aviation Administration (FAA) Aeronautical Fixed Telecommunication Network (AFTN) is used to communicate with MCCs and SPOCs
  - Over an MCI network is used to communicate with MCCs and SPOCs

Fascimile ~~thought~~ Faxman or through the MCI SAFE system is used to

Deleted: throught

- communicate with SPOCs and as a backup communications method for USCG RCCs
- Telex over the MCI SAFE system is used to communicate with the MCCs and SPOCs.
- FTP is used to communicate with CEMSCS

The USMCC exchanges data with MCCs, RCCs, LUTs and SPOCs in ASCII format. The USMCC binary data is from CEMSCS.

The communication function obtains configuration information from SQL configuration tables that is needed to receive data or to connect to a specific destination in order to transmit data.

The communications function converts data between internal USMCC format and external format. For example, MCCs use Julian dates, RCCs use year/month/date, but the USMCC stores dates in SQL date format. Binary files are used to stage input/output data and are described in the Baseline Document. Figures 2-2 through 2-4 detail the communication interface at the LUTs and RCCs.Figures 2-5 and 2-6 detail the communications at the USMCC.

Data exchange via the Internet uses FTP over VPN. Input data is processed from a local FTP server, and output data is placed on a remote FTP server. The input converter writes all inbound data to SQL based in put message tables for further USMCC processing. The output converter reads SQL based output message tables and formats the data for transmission from the USMCC.

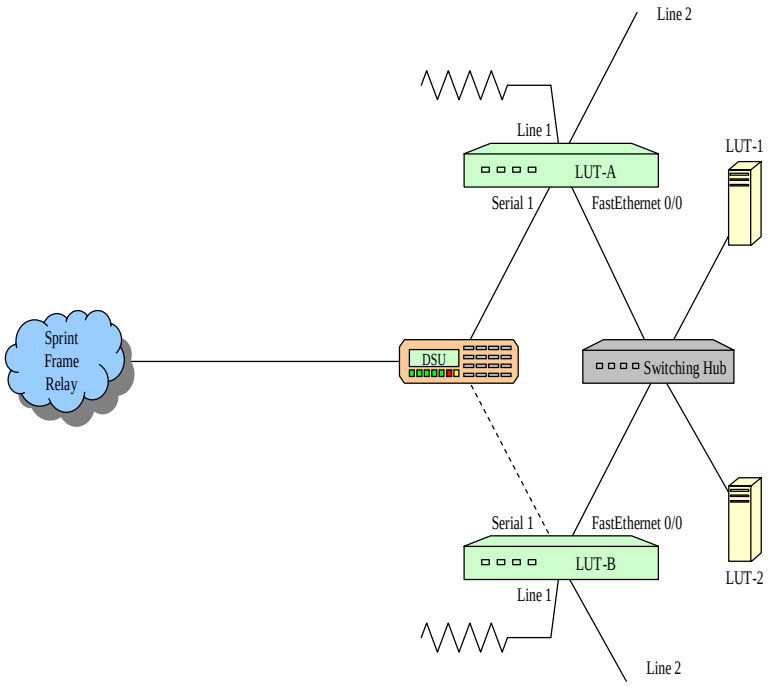

Figure 2-2: LUT Physical Network

United States Coast Guard Rescue Coordination Center Communication Description

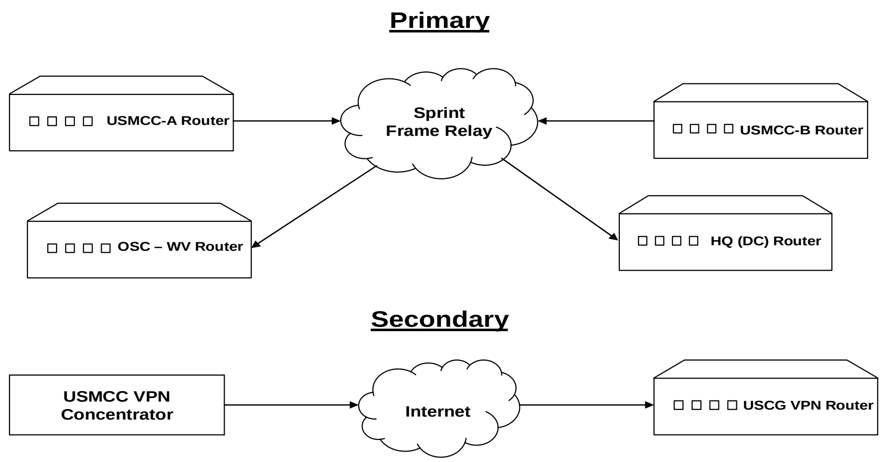

Figure 2-3: USCG RCC Communication Description

~~~~~~

Air Force Rescue Coordination Center Communication Description

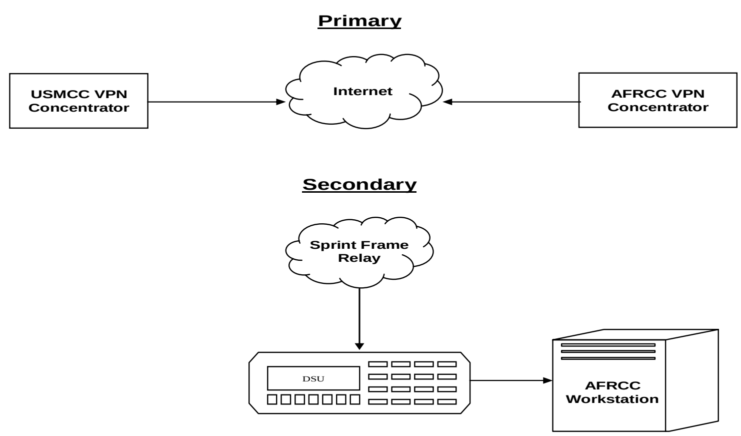

Figure 2-4: AFRCC Communication Description

8/3/05
~~~~~~

2.2.3 Operator Interface

The Operator Interface provides the tools that the Duty Controller uses to monitor and control the USMCC processes. All screens that are described below are available to any authorized user, including users who are not Controllers.

The main Operator Interface functions are:

- Controller log
- Operator message log and message log query;
- Alert site query and control ;
- Message query;
- Communications status and control;
- LUT pass monitoring;
- LUT control;
- Generate support messages;
- Morning briefing;
- Communication point of contact query;
- Large Location Error Analysis; and,
- Configuration control interface..

Each Operator Interface screen has two menu selections: "Connect" and "Print". These selections are located in the upper left hand corner of the screen, immediately below the title bar. The Connect selection is used to identify the database that the screen will use (such as Operational, Test, Developer and Archive). The Print selection allows the contents of the displayed menu window to be printed. Printer output will be to the default printer for the workstation that is running the program.

The operator interface screens were implemented using common Microsoft windows practices. A detailed functional description can be found in the Operator Interface Details document.

2.2.3.1 Controller Log

This interface allows Controllers and other users to log important events regarding the operation of the USMCC..

2.2.3.2 Operator Message Log and Message Log Query

The various USMCC processes/modules log messages for review. These messages describe the current state of the process and/or any unusual conditions that are encountered during processing. Each message is assigned a numerical value between 0 and 49 for programming priority and operations priority. The former is to assist programmers and software maintenance personnel in troubleshooting conditions that lead up to a problem; the latter is used to prioritize problems for USMCC Controller consideration/action. Messages with high operations priority are considered to be alarms and require acknowledgment by the Duty Controller. The series of tables that are

used for this function are described in detail in the Data Structures Document.

The Scroll module displays messages that scroll by on the Duty Controller screen and alerts the Controller to high priority messages. High priority system messages require USMCC Controller acknowledgment. When the USMCC Controller acknowledges a message, the time and user identification is recorded in the database.

The volume of messages produced for display is very high. To assist the Duty Controller in locating messages, a second program called OpQuery is provided. This program will search the operator log by subsystem (default is All), by programmer priority and/or operator priority (default with operator priority equal to or greater than 20), time range (default is the last 2 hours), message string and message number range. In addition, predefined groups of messages associated with certain processes or errors can be selected.

These modules require that the SQL server is working. A third module notifies the USMCC Controller when a program cannot access the SQL server.

2.2.3.3 Alert Site query and control (AlertSiteQuery)

The locations of active beacons are stored as Alert Sites. Each Alert Site is assigned a unique number and is linked to historical data that is associated with that beacon activation. This operator interface screen allows the user to query basic site information based upon site status-(open/closed), site id (site number or 406 beacon information), time range, site frequency, whether composite sites or all sites are displayed, and/or location constraints.

The Controller may query a site for information based on a defined geographical area, site frequency, site status, defined time period, and/or beacon identification code. The information returned provides the controller with details concerning the alert location, responsible SRR(s), source of the alert information (LUT and satellite), beacon identification or frequency, time of first and last site updates, or time and reason for site closure for historical data. Links are also available to source/destination messages that result from site activity.

After a site search query is done, a short list of site information is displayed in a window at the bottom of the screen. Selecting a specific site in this window will display an additional “Site Functions” screen. This screen is a Tab Box and the functionality is selected by clicking the appropriate tab:

- Site and SRR Status. This screen shows the SRRs for the site and their status. The user may change the message disposition for a particular SRR (destination), to make a SRR the primary or secondary destination for an alert site, or to restrict or expand the number of messages sent for an alert site. The user may also change the site status (Hold Open or Close). Modifications to the site are recorded in a change log along with the time of the change, person making the change and reason for the change.
- Summary Report. This provides a summary of information at the Alert site level.

- Intermediate Report. This option produces a summary of search results together with details for each pass on which the beacon was detected.

Each report may be printed or sent to a specific destination.

2.2.3.4 Message Query (MsgQuery)

This interface is used to retrieve either incoming or outgoing messages for viewing, printing and/or transmission. Messages are categorized by Type of Site (MCCs, SPOCs, RCCs, LUTs, CEMSCS, or Unknown). Messages may be selected by the type of site, specific destination (or all), incoming or outgoing, Message Type (Subject Indicator Type per C/S A.002 and LUT NTS), and/or time range (default is the most recent four hours).

When a message query is performed, the user is provided with a short summary list of messages that met the search criteria. The user may then select one or more messages from the list for further action. A selected message can be transmitted in the appropriate format to another MCC, RCC or SPOC by selecting the appropriate entries in the drop down list boxes under "Send To:". Message details can be viewed by selecting the desired message(s) and clicking the "Display" button. This action will bring up a new window that displays the entire contents of the message. A print button at the bottom of this window allows the contents of the display window to be printed.

2.2.3.5 Communications Status and Control (ComSiteDisplay)

This interface is used to monitor and control communications. This program initially presents the controller with a screen that is composed of two tabbed selections: 1) Communications Status; or, 2) Modify Com Site.

The Communication Status screen requires the user to select a tab for the type of communication site (MCC, RCC, SPOC, LUT or CEMSCS) to be displayed. The tab selection will produce a detailed listing of information pertaining to all sites of the type of site that was selected. Key information includes site name, path name, on line status and time/message number for the last communications exchange. Color coding is implemented to identify significant information.

The Modify Com Site screen is used by the Duty Controller to modify communications for a specific destination. The type of site and specific site are selected by using drop down list boxes that cause the current path and settings to be displayed. The Controller may then select an alternate path from a second display window or alter settings concerning the site status and the disposition of input and output messages for the site. The Controller must provide a brief explanation for each change. An alternative information window is provided to record tracking information such as ticket number used by the communication provider. A window at the bottom of this screen allows the user to view the recent history of changes made to the selected site.

A further selection allows controllers to view detailed information on a particular communication site. The selection called Launch ComCard Interface providers 24 hour contact, names and addresses, among the additional information.

2.2.3.5 LUT Scheduling and Interface

LutInterface is the main module that is used to control US LUTs. This screen allows the Duty Controller to:

- request a status message, schedule or pass data from a LUT
- send an MCC status, orbit vectors, LUT schedule, SARP Time Calibration (Tcal) message, or communications test message
- change a LUT schedule (track or suppress specific passes)
- activate the transfer of graphic files from a LUT to the USMCC (future enhancement), or
- allow specific LUTs or satellites to be excluded from use for missed pass calculations by frequency band(s)
- Request the LUT to send data to an alternate MCC (eg., the offsite USMCC)
- control the graphics display computers output (a future enhancement)

Formatted: Bullets and Numbering

Deleted: enchancement

Changes to next pass/missed pass and to a LUT schedule require the Duty Controller to enter a note explaining the change. LUT schedule changes are protected in order to avoid alteration by unauthorized users.

2.2.3.6 LUT Pass Scheduling (Pass Schedule)

PassSchedule is a complimentary module that is used to monitor LUT pass processing. It is based upon the USMCC schedule for all LUTs. Using default settings, the screen will display the past two hours and the next two hours for all scheduled LUT passes. The user may select a specific LUT, a pair of co-located LUTs, satellite, the time period, and display all passes, problem passes or scheduled passes. For each satellite pass that was scheduled or tracked by a LUT, a summary of results is displayed. This summary includes the satellite AOS and LOS times, the time that the MCC processed the data, the number of solutions received on each frequency band and observed anomalies such as a discrepancy between the number of solutions reported by the LUT versus the actual number that were received.

2.2.3.7 Generate Support Messages

“SupportMessages is used to create and transmit four types of narrative messages. These are the generic narrative messages (SIT 915 to MCCs and SPOCs and SIT 950 to U.S. RCCs), 406 MHz Registration Database message (SIT 925, System Status narrative message (SIT 605) and Next Visibility message (SIT 953). The 406 MHz registration database interface allows the user to enter criteria that can be used to search the 406 database. This information can then be inserted into a SIT 925 message. The next visibility function allows the user to enter criteria for the calculation of the next time of beacon visibility for a specified location.

2.2.3.8 Morning Briefing (MBrief)

MBrief collects information that is used for the morning briefing. It provides data on 406 MHz beacon activations located in a U.S. Search and Rescue Region (SRR). Information is presented by calendar day based upon the time at which a 406 MHz alert site is closed. Many data fields are extracted from the 406 MHz alert site summary table. Data fields that require user input are highlighted in yellow.

2.2.3.9 Configuration Control Interface (CCI)

Some limited recording of configuration changes occurs when actions are performed by the Duty Controller. These were described under previous sections.

2.2.4 System Data

System Data provides information that is critical to the proper functioning of the Cospas-Sarsat ground system. System data is exchanged primarily among Cospas-Sarsat Mission Control Centers. There are three different types of system data: 1) status messages that are exchanged among MCCs; 2) satellite orbit vector and time calibration data; and, 3) space segment provider messages.

2.2.4.1 System Status

The Cospas-Sarsat ground segment must function reliably and efficiently if Search and Rescue authorities are to receive distress alert data in a timely manner. Each MCC is responsible for monitoring its portion of the ground segment. In the event that significant changes occur in either the space or ground segments, system status messages are used to notify other MCCs. Nodal MCCs, such as the USMCC, may be required to inform several MCCs of any such changes. This is accomplished by using System Status messages. If the USMCC receives a System Status message, an alarm is passed to the Operator Interface to alert the USMCC Controller. This alarm must be acknowledged by the USMCC Controller. System Status messages received by the USMCC are automatically forwarded to other MCCs, using the nodal data distribution system. A separate software module allows the Duty Controller to create and send a System Status message. Procedures for handling system status are described in C/S A.001.

Deleted: automaticall

2.2.4.2 Orbit Vectors and Time Calibration

LUTs require accurate orbit vector information in order to track satellites and to compute accurate Doppler locations. The USMCC retrieves orbit vector information from the US Navy Bulletin Board for NOAA TIROS, Russian Nadezhda and other Cospar-Sarsat satellites. The USMCC validates input orbit vectors and sends them to other MCCs using the orbit vector message as described in C/S A.002. Orbit vectors are forwarded to USA LUTs twice daily at

preset times using NTS format. The USMCC Controller may update orbit vectors for any United States LUT using the LUT control interface described in 2.2.3.5.

Time Calibration (TCAL) information is needed by the LUTs to process 406 MHz data that is received from the SARP processor onboard Sarsat spacecraft. The TCAL message contains data about the spacecraft oscillator frequency and the rollover time of the onboard clock, which allows the LUT to translate the onboard time associated with alert data into co-ordinated Universal Time (UTC). TCAL information is received from France, validated at the USMCC and distributed to other Cospas-Sarsat MCCs in the Western DDR in the format described in C/S A.002. The Duty Controller can send TCAL to a USA LUT manually, using the LUT control Interface.

The routing of orbit vectors and Time Calibration data is determined by configuration in SQL tables. A more detailed description is provided in the Data Structures Document.

2.2.4.3 Space Segment Monitoring

Each space segment provider monitors and controls its own satellite equipment. If critical changes occur with satellites, other MCCs will be notified using system status messages (described above).

If status changes involve Cospas satellites, the Russian MCC (CMC) will notify other MCCs using system data distribution procedures described in C/S A.001.

The Sarsat space segment involves equipment from three different nations. Thus, the process is more complex. Canada provides the instruments for the Search and Rescue Repeaters (SARR) and the downlink transmitter. France provides the instruments for the Search and Rescue Processor (SARP). NOAA controls the satellite on which these instruments are carried. NOAA also receives and processes telemetry information, which is used to monitor the health of these instruments.

As various SARSAT satellites are tracked, telemetry information is received at CEMSCS. Information pertaining to SARSAT instruments is extracted and forwarded to the USMCC where data is stored in appropriate SQL tables. Limited statistical processing is carried out (minimum, maximum, average values) and included in summary messages that are sent to Canada and France. A SARR summary message is sent to Canada for each satellite daily. A SARP summary message is sent to France for each satellite monthly.

In addition to routine telemetry messages, special messages are used to report critical problems. Should a particular instrument report a value that falls outside predefined acceptable limits, an “Out of Limits” message is sent to the appropriate nation. When such a condition arises, an alarm is also sent to the Duty Controller at the USMCC.

The third aspect of space segment monitoring and control involves commanding the satellites to

alter their configuration based on space segment commands and procedures defined in the TCP. When such a message is received from Canada for SARR instruments or from France for SARP instruments, it is forwarded to the NOAA SOCC which schedules the command for execution. Once NOAA SOCC schedules a spacecraft command, it notifies the USMCC (via email), and the

USMCC sends a "Command Scheduled" message to the appropriate nation. Once NOAA SOCC executes a spacecraft command, it notifies the USMCC (via email), and the USMCC sends a "Command Verification" message to the appropriate nation.

Message formats for this data are described in C/S A.002, Cospas-Sarsat Standard Interface Description and the Telemetry and Command Procedures. The Data Structures Document describes the SQL tables that store this data in the USMCC..

Deleted: TheData

2.2.4.4 Pass Scheduling

Each day, the USMCC generates a 48 hour pass schedule for the USA LUTs. This schedule uses the most current orbit vectors, LUT and satellite configuration, and satellite tracking priorities that are stored in ASCII files. The schedules are written to ASCII files using MS Fortran. The schedules are transferred to the SQL database and then passed to the communication process for transmission to US LUTs.

2.2.5 System Monitoring (SMON)

This function detects possible malfunctions in the Cospas-Sarsat system and in the USMCC and brings them to the Controllers attention immediately. This function is carried out in near realtime and comprises six sub-functions.

2.2.5.1 LUT Pass Check

This check is performed each time a pass is received. Pass, Summary messages, solution headers and solution, data received from the LUTs are examined for time of receipt and content. by the USMCC controller using the "Pass Schedule" interface. Completed passes are correlated with USMCC Pass Schedules sent to the LUT and checked for:

- LUT status indicators,
- time of completion,
- number of solutions (121.5-MHz, 243-MHz, 406 interferers, 406 MHz PDS, 406 MHz SARR),
- LOS, and
- AOS.

Missing, late, incomplete and unscheduled passes, cause a message to the operator. The severity level of the message is determined by the nature of the discrepancy in the check.

2.2.5.2 LUT Orbit Vector Check

The LUT sends orbit vectors to the USMCC in response to orbit vectors sent by the USMCC and as part of LUT pass processing. The orbit vectors sent to the USMCC are verified against vectors at the USMCC. When orbit vectors are out of tolerance, an alarm is raised to the USMCC controller, so that accurate orbit vectors can be sent to the appropriate LUTs.

2.2.5.3 LUT Beacon Location Accuracy Check

In a future enhancement, solutions from the US LUTs will be scanned for known test and orbitography beacons. Locations in error by more than a nominal distance will cause an alarm to be raised to the USMCC controller and also be written to a Location Error file for future reference and analysis. This enhancement will utilize software written for Large Location Error monitoring. Location errors identified by this check may indicate a LUT problem that can be resolved by Controller procedures.

2.2.5.4 LUT Communications Check

No special automated check of LUT communications is currently performed at the USMCC.

2.2.5.5 MCC Processing Checks

A set of stored procedures in the SQL Database are regularly activated in order to verify MCC processing. These procedures check:

(1) time expired since last USMCC output alert message;
(2) time to complete processing of USMCC input data;
(3) time since last input to USMCC by an MCC;
(4) time for processing of Alert data from US LUTs; and
(5) Time for sending data from the USMCC.

Out-of-tolerance conditions are reported to the USMCC Controller..

2.2.5.6 Large Location Error Check

This process automatically extracts all 406-MHz location errors greater than 120 kilometers. Large Location errors are reported each day according to Cospas/Sarsat procedures. A user interface is provided (LLE.exe) for system analysts where data is also analyzed manually by comparison with SAR reports from RCCs and other sources. Unlike the Beacon Location Accuracy check (2.2.5.3), this check is only applied to operational beacons. Data is ultimately translated from SQL tables to a Microsoft Access format and this output is provided as a quarterly report to the Cospas-Sarsat Secretariat (conversion etc. provided by LLEAccessReport. exe).

2.2.6 406 Registration Database (406 RGDB)

When United States coded beacons are purchased by users, additional information is provided by the owner and recorded in a database for use by Search and Rescue Forces. This process is referred to as beacon registration. The 406 Registration Database (RGDB) is managed by NOAA/NESDIS at the USMCC facility. The format for registration data varies based on the type of beacon registered. Emergency Position Indicating Radio Beacons (EPIRB) for vessels, Emergency Locator Transmitters (ELT) for aircraft, and Personal Locator Beacons (PLB), have different formats. Examples of these formats may be found in Appendix 2 to the USMCC National RCC and SPOC Alert and Support Messages document.

When the USMCC receives a 406 beacon alert, some of the beacon information is decoded and stored in the alert database tables. The 15 character hexadecimal identifier of the beacon is then used to access the RGDB to obtain additional information about the owner, vehicle identification, etc. This information is attached to alert messages that are sent to RCCs. If a USA registered beacon is activated in an area outside the USA AOR, the USMCC Controller can access the database, using the beacon identification code, and forward registration information to appropriate search and rescue authorities when requested, using a SIT 925 message format (2.2.3.6).

Information is provided in the RGDB such as owners name, mailing address, telephone numbers for the owner, points of contact, vessel name, type, size, capacity, radio call sign, registration number, communications equipment, home base.

An Web based application is provided for beacon owners to enter and modify registration information. When registration information is received via postal mail or facsimile it is manually entered into the RGDB by NOAA personnel using the same application. The information is stored in an SQL database. After a beacon is registered in the database, update reports are generated and sent to each owner to confirm that the beacon was registered and provided the associated data for their review. Other mailings involve decals that need to be affixed to owner's beacon. Additionally, every two years, owners are contacted in order to verify that registration information is correct and up to date. The RGDB is used in conjunction with the IHDB (discussed below) to monitor overall effectiveness of 406 beacons.

2.2.7 Incident History Database (IHDB)

The IHDB is used to generate national and international reports, and to identify opportunities to improve beacon design, regulation, information processing and alert response. The Air Force, Coast Guard, and NOAA have worked together to establish the minimum information required to improve the system. The current Incident History Database is connected to a Web Application that Search and Rescue Forces can use to update case information through the internet.

When the USMCC resolves ambiguity for a 121/243 MHz site and the composite location lies within the US AOR, an incident feedback report is attached to the site information for

transmission to an RCC. This form requests information from the RCCs on the outcome of distress signals which is only available at the RCC. USMCC provided information includes Site ID, time that the composite location was detected and its calculated latitude and longitude. When a site closes, USMCC software adds the site information to the IHDB if appropriate. Since the IHDB is on a different domain than the MCC the data must be sent through COMM and a program on the Web domain reads and inserts the data into the IHDB.

For 406 MHz beacons, as well, data is written to the IHDB when the composite location is within the US AOR. In addition, data is written to the IHDB for unresolved 406 MHz alert sites where one location lies within the US AOR. The Site ID, the location associated times, the 15 hexadecimal Beacon Identification code, beacon manufacturer, beacon model and beacon type are written to the IHDB. Additional encoded information included in the Incident Report is the Beacon Identification code (15 hexadecimal), Manufacturer, Model and Type are written to the IHDB.

Information provided by RCCs includes the role that Cospas-Sarsat alert data played in the incident, RCC mission numbers, number of people saved, resources involved, mission status (distress/non-distress), time line information, actual location and reason for beacon activation. The RCCs can enter this information over the internet by accessing the IHDB Web Application. Information from the morning report to NOAA is also used to update the IHDB. These processes are partially automated, and are described in the FRD. Future work will focus on further automating external (RCC) inputs to the IHDB process.

Periodic reports are produced from the IHDB. These include information sent to 406 MHz beacon manufacturers concerning beacon activations in distress and non distress situations. Similar reports are provided to US RCCs each quarter and annually to the Cospas-Sarsat Secretariat.

2.2.8 Self-Test And Monitoring System

2.2.8.1 General

The Self-test and Monitoring System monitors the satellites, LUTs, orbitography beacons, and LUT-MCC operations. SAMS monitors availability (which components are working), performance (how well they are working) and activity level (how many beacons the system is handling). While SMON monitors for realtime errors, SAMS is more oriented towards identifying longer term trends.

The SAMS provides enough history to detect failure patterns and performance trends for medium and long term monitoring. It is not intended to provide the rapid response information needed for failure detection and repair on a near real time or day-to-day basis, which is provided by the Real-Time System Monitoring function.

2.2.8.2 Data

Data for SAMS trend reports are obtained from the Alert Processing, System Data, and Communication subsystems. The data cover satellites, orbitography beacons, and US LUTs. SAMS collects and stores data every day and displays them on a 30-day time line. SAMS is updated overnight and is made available by 9:00 AM local time. The displays are both graphical and tabular. Users may access the last day's information at any time.

2.2.8.3 Operation

SAMS is created on a PC which downloads its data from the operational USMCC SQL Database at 0600 UTC each day. The SAMS PC prepares plots and reports every morning so that they are available to the local terminals by 1400 UTC. The monitoring period covered by the data is the thirty days ending at the last UTC midnight.

2.2.8.4 Exceptions Reports

The Exceptions Report provides a brief summary of instances meeting certain exception criteria. Review of the Exceptions Report provides a rapid overview of unusual system operations in the last 30 days. The report may be printed after viewing.

2.2.8.5 Availability

The availability plots' in SAMS measure the availability of LUTs, satellites, and selected orbitography beacons during the preceding 30 days.

(1) LUTs: The Single LUTs menu selection displays information for each of the 12 LEO LUT considered independently. The plots shown under "Dual LUTs" are the same as those for "Single LUTs", except that the two LUT at a site are treated as a single unit. Thus a pass is considered to be completed by the combined LUT if it is completed by either LUT, and not completed only if neither LUT completes it.

(2) Satellites: Satellite availability is measured by its 406-MHz burst message throughput. This is defined for each pass over an orbitography beacon as the number of beacon burst messages transmitted out of the satellite, divided by the number received by the satellite, times 100. Practically, the number out of the satellite is taken to be the maximum number of bursts recorded by any of the US LUTs, and the number into the satellite is determined by dividing the time from first to last point by the orbitography beacon period, and adding one. Average throughput is displayed in SAMS by day over the last thirty days for each satellite and beacon.

(3) Beacons: These plots provide an overview of burst reception from each 406 MHz orbitography beacon over the last 30 days.

2.2.8.6 Performance

The Performance plots in SAMS measure location accuracy and system timing during the preceding 30 days.

Location Accuracy

(1) SAMS derives the location accuracy of operational 121.5/243-MHz beacons from all alert sites that have been closed in the thirty days prior to GMT midnight. Location accuracy is based on the site and pass composites.

(2) The location accuracy of operational 406-MHz beacons shown is derived by SAMS from all Alert Sites that have been closed in the thirty days prior to GMT midnight. The data are derived from the USMCC Alert Site File. Location accuracy is based on the site and pass composites.

(3) SAMS displays the orbitography beacon location errors in various formats in order to help identify the error sources. The formats are:

(A) Scatter Plots by LUT, by satellite, and by orbitography beacon. These show the location error in kilometers in the east and north directions.

(B) Daily Plots by LUT and satellite, giving the average error by day for errors under 10 kilometers.

(C) by Pass Parameters: number of points, curve duration, elevation angle, central angle, measurement noise, A-Probability, window factor, frequency bias, bias standard deviation, satellite, LUT and MCC.

(D) by quality filter. These plots show the percent of errors greater than 5 kilometers by LUT, satellite, and beacon for solutions with three or more points, window factor between -1 and +1, and Central Tracking Angle (CTA) between 1 and 30 degrees.

System Timing

(1) LUT processing time is the time from satellite loss of signal (LOS) time to LUT pass processing complete time (LPC), as reported by the LUT in the Pass Summary message. It is shown by SAMS for the US LUTs in a set of four plots covering the last 30 days.

(2) LUT-MCC communication time is the time from LUT processing complete, as reported in the Pass Summary message, to the time the last message for the pass was received by the USMCC. A set of four screens shows communication time for each of the LUTs over the last 30 days.

(3) The MCC Processing Times plot shows, in the upper half, the times from first receipt at the MCC to first send from the MCC, for each LUT pass during the preceding 30 days. The lower half of the screen shows the time from receipt of the last data for a LUT pass to the time the MCC processing is complete for that pass.

2.2.8.7 SAR Activity

The SAR Activities plots in SAMS are intended to display various measures of SARSAT operations volume directly related to Search and Rescue messages and sites. Five plots are implemented.

Messages

(1) Messages Sent - Last 30 Days: This plot shows the number of messages per day sent out of the USMCC, by destination, averaged over the last 30 days. The destination categories are US RCCs, SPOCs, MCCs, LUTs, Others. Method of transmission is shown as X.25 for PSDN, TELX for TELEX, FAX, and OTHER for all other.

(2) Messages to RCCs: This is a single plot showing the time history of messages to the US RCCs over the last 30 days. All message types are counted. Each bar represents the number of messages sent in the day.

(3) Messages to SPOCs, MCCs, LUTs, and Others: These three plots are similar to those for the preceding, except for the destination groups.

Active Sites

Two plots for 121.5/243-MHz Sites are derived from Alert Sites closed in the last 30 days. The first shows the number of sites closed in each day, broken down by the number of passes per site. The second shows the same time history broken down by beacon frequency. Two plots for 406-MHz Sites show the number of sites closed in the last 30 days, broken down by site multiplicity (first screen) and by beacon protocol (second screen).

2.2.8.8 Statistical Reports

This menu item provides access to the data underlying the SAMS plots. The reports may be viewed or printed. The following reports are provided:

- LUT Pass Schedules
- LUT and MCC Timing
- Orbitography Beacon Errors Less than 120 kilometers
- Orbitography Beacon Errors less than 10 KM
- Orbitography Beacon Periods
- Solution Filter Statistics
- Orbitography Beacon Missing Points and Errors at US LUTs
- Orbitography Beacon Location Error Distributions by Pass Parameter
- 406 MHz Location Error Distributions
- 121/243 Active Site Summary Tables
- 406 Active Site Summary Tables

2.2.9 LUT Monitoring Data Base

LUT passes are monitored daily to compile a monthly LUT summary for contractual purposes. The software executes every day, compiling data for the previous day. The data accumulate indefinitely. The software provides four types of report and two operator sub-functions.

2.2.9.1 LUT Maintenance Report

This report is a monthly summary of missed and successful passes for contractual purposes. It lists scheduled passes, missed passes, and the payment schedule.

2.2.9.2 LUT Availability Reports

The LUT Availability Reports provide availability data (scheduled passes, missed passes) for either single LUTs or for LUT sites (pairs at one location). The user may select the time period covered: (1) last 12 months; (2) year to date; (3) previous year; (4) last quarter; (5) last two quarters; (6) last four quarters; or, (7) a manually entered date.

2.2.9.3 LUT Daily Pass Summary

This function provides a summary of availability and accuracy of the US LUTs for any interval of days. The report includes scheduled and missed passes, number of location errors, number of solutions by frequency, LUT processing time and LUT-MCC transfer time.

2.2.9.4 Operator Logging of Missed Passes

This function allows the Controller to log missed passes for any LUT. The Duty Controller inserts satellite, orbit number, LUT, and reason for the missed pass.

2.2.9.5 Operator Charge or Excuse Missed Passes

This function enables LUT passes to be charged or excused manually, which affects the payment to the LUT maintenance contractor.. The purpose of the function is to allow manual adjustment of the LUT Missed Pass Reports based on data and conditions not known by the automated system. Access is restricted to authorized personnel; some changes are made by the USMCC Controller and some changes made by NOAA personnel.

Deleted: ¶

2.2.10 Interference Monitoring

The frequency spectrum between 406.000 - 406.100 MHz has been reserved by the International Telecommunications Union for the use of emergency beacons transmitting in the earth to space direction. Nevertheless, some earlier users have not vacated this portion of the spectrum, and new users appear from time to time. Non-distress signals that are present in this portion of the

spectrum (or strong signals adjacent to this band) can affect the ability of the spacecraft instruments to detect distress beacons. Non-distress signals are termed interference. Cospas-Sarsat monitors this portion of the spectrum in order to identify and locate interfering signals.

Interfering signals that are located in the USA Service Area by other Cospas-Sarsat providers are forwarded to the USMCC using SIT 121 messages formats. These messages are processed and stored in special database tables on the SQL server. USA LUTs can also be configured to locate interfering signals. Doppler information from the signal is used to calculate the location of the interfering signal.

Interference Processing, provided by intf.exe, of these Doppler locations is essentially identical to the Alert Processing for 121.5/243-MHz transmitters discussed in Section 2.2.1. Interference signals for locations outside the USA Service Area generate SIT 121 messages to other MCCs (standard filtering to prevent redundant messages is applied) and signals inside result to messages to the Federal Communications Commission (FCC). The creation of a message to the FCC is very limited and controlled by configuration parameters stored in the SQL database. Finally, the INTF software also produces a daily report of interference activity (sent as an internal message) which is reviewed by a systems analyst.

An additional application is provided for systems analysts to support interference monitoring. A user interface (INTFInterface.exe) allows for review of data, plotting of data on a map, maintaining a history of data and reprocessing of data. This application also provides mechanisms that automate the process and assist in producing a quarterly report of interference activity for the Cospas-Sarsat Secretariat.

Although the Sarsat SARR repeater is the main instrument used to locate interference, later generation Sarsat SARP instruments have been modified to assist in this task. This method uses pseudo-codes in the 406 messages to report interference. Future software may be added to process these messages.

A definition of the SIT 121 message format is provided in C/S A.002. A definition of the 406 Interference message format that is sent to the MCC by LUTs is provided in the LUT Data Transfer Specification (DTS). A description of the SQL tables is provided in the Data Structures document.

2.2.11 Database Maintenance

The database maintenance subsystem is used to archive, purge and backup data and to monitor database performance.

2.2.11.1 Archive/Purge

The archive/purge functions reside on the SQL server where the database resides. Archiving is launched by SQL executive once per minute. It transfers any data that is more than 60 days old

to the archive database and removes all corresponding files from the operational database.

2.2.11.2 Backup

For backup purposes, three software packages are used: 1) Seagate Backup Executive for Windows NT; 2) SQL Agent add-on; and 3) the Open File option. Backup is run daily for all shared files (MccNet and USMCC workstations), all NetWare volumes, and for the operational database, archive database and tables in the operational database. Backup is made to 4mm DAT cassettes with a 24 GB capacity.

2.2.11.3 Monitoring

The database is monitored for security, throughput, speed, capacity problems. Some database tools were provided with SQL software to troubleshoot problems after the fact. Future development will focus on software packages that can provide advance warning of problems such as a security penetration, low capacity, problems running archive/purge, and so forth. The goal will be to detect problems before a failure occurs.

2.2.12 SAR Mapping and Geosort

MapInfo mapping software is used to provide the Controllers with visual maps and to define, maintain and modify boundaries for geographical regions that are used by the Alert Processing subsystem. MapInfo software is resident on the MccDisplay workstation.

Some MapInfo capabilities are used for viewing, such as zoom in/out. A custom USMCC program ("MapDisplay.exe") allows the user to select what is displayed and defines map symbols that are used. This program displays information on the map for open 121/243 MHz and 406 MHz sites. Clicking on a site will highlight unresolved site A-B solutions. The map display can only be run on Display.

3.0 Hardware Functional Description

Topology diagrams for the various USMCC networks are provided in Section 1. The system uses Microsoft 2003 network capabilities. The equipment described below (except for the USMCC remote offsite network) is located in racks in the operations room on the fourth floor of the NOAA Satellite Operations Facility (NSOF)

3.1 USMCC Network

a. Cisco 3020 VPN Concentrator - Provides the capability to communicate over the internet through a virtual private network (VPN)

b. HP ProCurve Unmanaged Hub 12 port (J3294A) - connects the outside interface of the Cisco Pix firewall.

c. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports.

d. Cisco PIX 525E Firewall w/ Failover - Provides protection from unauthorized access to the USMCC network.

3.1.1 MCC DMZ

a. MCCFTP1 - This server:

- acts as the FTP server for USMCC communications with foreign MCCs, CEMSCS and appropriate RCCs and SPOCs
- acts as the FTP server for transfer of data between the USMCC and the web applications network (RGDB and IHDB).
- Retrieves orbit vectors from the Naval Bulletin Board
- Acts as a fax server for the USMCC fax communication option.

b. MCCFTP2 - This server provides identical functionality as MCCFTP1. It acts as prime backup and provides a parallel testing capability.

c. FTPIDS - This server provides intrusion detection for the MCC DMZ segment as well as network monitoring.

d. FTPMonitor - This server provides network monitoring, antivirus maintenance and patch management functions for the MCC DMZ segment.

e. Cisco Router 2600 - This router, called "MCC-FAX", is used to provide a modem bank for outgoing fax.

3.1.2 MCC Segment

a. HP Procurve 4000 switch - Layer 2 managed switch with 40 10/100 ports.

b. HP Procurve 2824 switch - Layer 2 managed switch with 20 10/100/1000 ports
c. MCCPrim - This server:
- acts as the primary domain controller for the MCC Segment
- acts as file server for the MCC Segment
- acts as WINS server to map addresses to servers/workstations

d. MCCProc1 - This server provides the core operational USMCC data processing functions including alert processing, LUT Monitoring, interferer processing, system monitoring, and task scheduling.

e. MCCDb1a /MCCDb1b - This set of redundant servers provides the USMCC database functionality for both the operational database (most recent 60 days of data) and the current archive database (current year). The attached RAID device provides the database storage.

f. MCCCom1 - This server
- handles USMCC communications including X.25, frame relay and AFTN communication services,
- processes telemetry data received from the UMSCC FTP server into the SQL database,
- provides the capability to convert data between external formats and the internal (SQL database) format
- contains an EICON card to connect commercial Packet Switching Data Networks (PSDN) for X.25 communications. Telex formatted messages are also sent to appropriate external gateways via X.25.
- provides communication task scheduling.

g. MCCOps1 - This server provides the interface between the duty controller and the USMCC. The Operator Interface software is used to monitor the daily operations of the USMCC.

h. MCCSec - This server acts as a backup to MCCPrimary and also provides Print Server capability for the MCC Segment.

i. MCCProc2 - This server provides identical functionality as MCCProcess1. It acts as prime backup and provides a parallel testing capability.

j. MCCDb2a/MCCDb2b - This set of servers provides identical functionality as MCCDb1 & 1a. It acts as prime backup and provides a parallel testing capability

k. MCCCom2 - This server provides identical functionality as MCCComm1. It acts as prime backup and provides a parallel testing capability

l. MCCOps2 - This server provides identical functionality as MCCOps1. It acts as prime backup and provides a parallel testing capability. It also monitors the daily operations of the test system.

m. Display - This server:
- processes data through the Self-test and Monitoring System (SAMS) and displays the results
- processes alert data through MapInfo mapping software and displays the results.

n. MCCAnalyzer - This server provides the capability to analyze X.25 traffic.

o. MCCIDS - This server provides intrusion detection for the MCC segment as well as network monitoring.

p. MCCMonitor - This server provides network monitoring, antivirus maintenance and patch management functions for the MCC segment.

q. BackupSrv - This server provides the capability to backup user files from the MCC segment.

r. Time - This server provides system timing derived from GPS. Correct synchronized timed is critical for the USMCC system operation.

s. Non-Internet Workstations – These provide access to the MCC network for Operations and maintenance personnel.

3.2 LUTServer Network

a. Cisco Pix 525E Firewall - Provides protection from unauthorized access to the LUTServer network.

3.2.1 LUT DMZ Segment

a. LUTFTP1 - This server acts as the FTP server for USMCC communications with US LUTs and Coast Guard RCCs.

b. LUTFTP2 - This server provides identical functionality as LUTFTP1. It acts as prime backup and provides a parallel testing capability.

c. HP Procurve 2824 Switch - Layer 2 managed switch with 20 10/100/1000 ports.

3.2.2 LUT INTRANET Segment

a. Cisco Router 2600 - This router, called "USMCC-A", is used to provide a connection to the Sarsat Sprint Frame Relay Network. This router provides CHAP protected dialed backup capability to the LUTs.

b. Cisco Router 2600 - This router, called "USMCC-B", is used to provide an additional connection to the Sarsat Sprint Frame Relay Network. This router provides CHAP protected dialed backup capability to the LUTs.

c. HP ProCurve 2824 Switch - Layer 2 managed switch with 20 10/100/1000 ports

3.2.3 LUTServer Segment

a. LUTSVR – provides capability to collect data from both operational and test LUTs solution data processing algorithms (Non-operational)

b. LSE - LEO Support Equipment – provides a test system for upgrades to LEOLut software.

c. GSE – GEO Support Equipment - provides a test system for upgrades to GEOLut software.

d. HP ProCurve 2824 Switch - Layer 2 managed switch with 20 10/100/1000 ports.

3.2.4 GEOLUT Segment

a. MDLUT1 – Operational Geostationary LUT

b. MDLUT2 - Operational Geostationary LUT

c. HP ProCurve 2824 Switch - Layer 2 managed switch with 20 10/100/1000 ports.

3.3 Web Applications Network

a. Cisco 3020 VPN Concentrator - provides the capability to communicate over the internet through a virtual private network (VPN).

b. HP ProCurve Hub 12 port (J3294A) - connects the outside interface of theCisco Pix firewall.

c. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports.

d. Cisco PIX 515E Firewall with Failover - provides protection from unauthorized access to the Web Applications network.

3.3.1 Web DMZ Segment

a. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports.

b. WEBSRV – This server is the main production web server that provides a web interface to the following production applications:

- RGDB
- IHDB
- Argos
- Direct Readout

Deleted: DirectReadout

c. WEBDRVDEV – This server is used as the testing web server that provides a web interface to the following test applications:

- RGDB
- IHDB
- Argos
- Direct Readout
- IBRD

Deleted: DirectReadout

d. RGDBFTP – This server provides functionality to FTP the RGDB web data located on APPSRV to the controller database located on the MCC domain.

3.3.2 Web Application Segment

a. Cisco PIX 515E Firewall with Failover - provides protection from unauthorized access to the Web Applications network.

b. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports

c. APPSRV - The main production application server that runs the Registration Database web software (RGDB). Connected to external RAID.

d. APPSRVDEV – This is the test application server. It contains the following applications:

- RGDB
- IHDB
- Argos
- Direct Readout
- IBRD

e. APPSRV2 – This server provides backup functionality for APPSRV. All backups of the RGDB and IHDB databases are run from this server using the Veritas Backup Exec software.

f. RGDBWS1 - This is the production application server that contains the following applications:

- IHDB
- Argos
- Direct Readout

Deleted: DirectReadOut

g. DC1 - This server provides the capability to copy jobs for RGDB and IHDB and for the daily count program (registrations processed over time) for the RGDB.

h. DC2 – This server acts as the Backup of DC1. The IDS console is run from here

i. NOAAIDS - This server provides intrusion detection for the web applications network as well as network monitoring.

j. Monitoring Server - This server provides network monitoring, antivirus maintenance and patch management functions for the web applications network.

k. Workstations - All the following workstations provide access to the MCC segment for our analysts, developers, maintenance, and data entry.

l. Decal Printer1 - Provides capability to print specialized decals required in the beacon registration process.

m. Decal Printer2 - Provides backup to DecalPrinter1

n. HP Printer 8000 - Provides printing capability for the web applications network.

3.4 Offsite Network

a. Cisco 3020 VPN Concentrator - Provides the capability to communicate over the internet through a virtual private network (VPN).

b. HP ProCurve Hub 12 port (J3294A) - connects the outside interface of theCisco Pix firewall.

c. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports.

d. Cisco PIX 515E Firewall with Failover - provides protection from unauthorized access to the Web Applications network.

3.4.1 Offsite DMZ Segment

a. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports.

b. MCCFTP3- This server:

- acts as the FTP server for USMCC Offsite network communications with foreign MCCs and appropriate RCCs and SPOCs
- acts as a fax server for the USMCC Offsite network fax communication option.

c. MCCINTERNET3 - This server provides internet access for controllers to send and receive e-mail related to USMCC operations while at the Offsite USMCC.

3.4.2 Offsite MCC Segment

a. Cisco Router 2600 - This router, called "USMCC-C", is used to provide a connection to the Sarsat Sprint Frame Relay Network.. This router provides CHAP protected dialed backup capability to the LUTs

b. HP ProCurve Switch 2824 - Layer 2 managed switch with 20 10/100/1000 ports

c. MCCPrim3 - This server:
- acts as the primary domain controller for the Backup MCC Segment
- acts as file server for the Backup MCC Segment
- acts as WINS server to map addresses to servers/workstations

d. MCCSec3 - This server acts as a backup to MCCPrim3 and also provides Print Server capability for the Backup MCC Segment.

e. MCCProcess3 - This server provides the core Backup MCC data processing functions including alert processing, LUT Monitoring, interferer processing, system monitoring, and task scheduling.

f. MCCDbs3 - This server provides the Backup MCC database functionality for both the operational database (most recent 60 days of data) and the current archive database (current year).

g. MCCOps3 - This server provides the interface between the duty controller and the Backup MCC. The Operator Interface software is used to monitor the daily operations of the Backup MCC.

h. MCCOps3-2 - This server acts as backup to MCCOps3

i. MCCComm3 - This server
- handles BackupMCC communications including X.25, frame relay and AFTN communication services,
- provides FTP service for telemetry processing,
- provides the capability to convert data between external formats and the internal (SQL database) format

- contains an EICON card to connect commercial Packet Switching Data Networks (PSDN) for X.25 communications. Telex formatted messages are also sent to appropriate external gateways via X.25.
- provides communication task scheduling

j. MCCIds3 - This server provides intrusion detection for the Backup MCC segment as well as network monitoring.

k. MCCMonitor3 - This server provides network monitoring, antivirus maintenance and patch management functions for the Backup MCC segment.

l. TimeSource - This server provides system timing derived from GPS. Correct synchronized timed is critical for the USMCC system operation.

m. Lexmark Printer - Provides printing capability for the Backup MCC Segment.